IN THE DISTRICT COURT OF THE UNITED STATES
FOR THE DISTRICT OF SOUTH CAROLINA
GREENVILLE DIVISION

UNITED STATES OF AMERICA, Plaintiff, vs. 0.24247794 BITCOIN (BTC), AND 38,616.40303284 TETHER CRYPTOCURRENCY (USDT) Defendant *in Rem*.	)	CIVIL ACTION NO.:

UNITED STATES' COMPLAINT FOR FORFEITURE *IN REM*

The Plaintiff, United States of America, brings this complaint and alleges as follows, in accordance with Rule G(2) of the Supplemental Rules for Admiralty and Maritime Claims and Asset Forfeiture Actions.

NATURE OF THE ACTION

1. This is a civil action *in rem* to forfeit to the United States of America funds in the amount of 0.24247794 Bitcoin ("BTC") and 38, 616.40303284 Tether Crypto Currency ("USDT") valued at approximately $43,871.85 USD ("United States Dollars"), ("Defendant Funds"), pursuant to 18 U.S.C. § 981(a)(1)(A) and 18 U.S.C. § 981(a)(1)(C). The United States seeks forfeiture based upon a reasonable belief that the Government will be able to meet its burden of proof at trial to show that the Defendant Funds constitutes, or is traceable to:

a. property involved in wire fraud transactions or attempted wire fraud transactions in violation of 18 U.S.C. § 1343

b. property involved in money laundering transactions or attempted transactions in violation of 18 U.S.C. § 1956(a)(1)(A)(i), and/or § 1956(a)(1)(B)(i) and/or 1957;

c. property involved in an illegal money transmitting business, in violation of 18 U.S.C. § 1960; and/or

d. proceeds of some other form of specified illegal activity set forth in 18 U.S.C. § 1956(c)(7) and;

e. proceeds of some other form of specified illegal activity set forth in 18 U.S.C. § 1956(h) and;

f. property involved in money transactions in criminally derived property or attempted money transactions, in violation of 18 U.S.C. § 1957.

JURISDICTION AND VENUE

2. This Court has subject matter jurisdiction over an action commenced by the United States pursuant to 28 U.S.C. § 1345, and over an action for forfeiture by virtue of 28 U.S.C. § 1355. This Court has *in rem* jurisdiction over the Defendant Funds pursuant to:

(a) 28 U.S.C. § 1355(b)(1)(A), because acts or omissions giving rise to the forfeiture occurred in the District of South Carolina; and

(b) 28 U.S.C. § 1355(b)(1)(B), because venue properly lies in this district pursuant to 28 U.S.C. § 1395.

THE DEFENDANT *IN REM*

3. The Defendant Funds consist of 0.24247794 BTC and 38, 616.40303284 Tether Crypto Currency USDT valued at approximately $43,871.85 USD, obtained by agents with the United States Secret Service ("USSS") during an investigation into a transnational criminal organization running an exploitation of elderly and social engineering scam. The funds were seized from a cryptocurrency custodial wallet under the control of Binance, identified by account number xxxxx8257 (the "Suspect Wallet 1") and under the name of Avinash Pal ("Pal").

4. The USSS seized the 0.24247794 Bitcoin BTC and 38, 616.40303284 Tether Crypto Currency USDT valued at approximately $43,871.85 USD, for federal forfeiture. The Defendant Funds are currently restrained and pending deposit to an account under the control of United States Secret Service.

5. In accordance with the provisions of 19 U.S.C. § 1606, the Defendant Funds have a total domestic value of approximately $43,871.85

KNOWN POTENTIAL CLAIMANTS

6. The known individuals whose interests may be affected by this litigation are:

a. Avinash Pal who may have an interest in the Defendant Funds because he was the named account holder of the account seized by USSS during this investigation.

BASIS FOR FORFEITURE

7. Pursuant to the pleading requirements of Supplemental Rule G(2)(f), Plaintiff alleges that there is a factual basis to support a reasonable belief that the Government will be able to meet its burden of proof at trial to show that the Defendant Funds are subject to forfeiture to the United States, based in part upon the following:

a. USSS and local law enforcement agencies were investigating a transnational criminal organization running an exploitation of elderly and social engineering scam. In brief summary, investigating agents determined that a scamming group has been using social engineering to contact elderly individuals and convince them that their bank accounts are compromised. Once the scammers have engagement from the victim, they instruct them that their bank accounts are compromised and that they need to put their funds in a secure location while they investigate. The victims then withdraw their funds in cash and take it to a BTC Automated Teller Machine ("ATM"). From that ATM, the funds are sent to a cryptocurrency wallet address provided by the suspects.

b. Digital currency (also known as virtual currency or cryptocurrency)[1] is generally defined as an electronic-sourced unit of value that can be used as a substitute for fiat currency (i.e., currency created and regulated by a government). Digital currencies exhibit properties similar to other currencies, but do not have a

[1] For purposes of this complaint, the terms "digital currency," "cryptocurrency," and "virtual currency" are used interchangeably and address the same concept.

physical form, existing entirely on the internet. Digital currency is not issued by any government or bank (in contrast with fiat or conventional currencies) and is instead generated and controlled through computer software operating on a decentralized peer-to-peer network, often referred to as the blockchain or public ledger. Digital currency is legal in the United States and accepted for legitimate financial transactions. However, digital currency is often used for conducting illegal transactions or for concealing or disguising the true nature, source, location, ownership or control of illegally obtained proceeds. Bitcoin ("BTC") is one of the most commonly used and well-known digital currencies. Ethereum ("ETH") is another popular and commonly used digital currency.

c. A stablecoin is a digital currency whose market value is attached to or "pegged" to another stable asset. Differing from normal digital currencies, the value of stablecoins are pegged to assets such as fiat currencies like the United States Dollar ("USD") or the Euro, or other types of assets like precious metals or other digital currencies. Stablecoins are thus used to mitigate the volatility in the price of digital currency by mimicking the value of a fiat currency, without actually converting digital currency into fiat. While there are various legitimate uses for stablecoins, they are popular with cyber-criminals who seek to hold digital currency proceeds of crime at a stable or near-fixed value without moving those funds into the legitimate financial system into a fiat currency such as USD. Some examples of stablecoins include:

a. Tether (USDT) was developed by Tether Limited Inc. and is designed to maintain its value at $1.00 USD. USDT can utilize the existing ETH blockchain or the newer TRON ("TRX") blockchain.

b. Binance USD (BUSD), which was developed by Binance Holdings Limited and Paxos Trust Company, LLC, is designed to maintain its value at $1.00 USD. BUSD utilizes the existing ETH blockchain.

d. A digital currency exchange (an "exchange") is a business that allows customers to trade digital currencies for other digital or fiat currencies. An exchange can be a brick-and-mortar business, or strictly an online business. Both brick and mortar and online exchanges accept a wide variety of digital currencies, and exchange them for fiat and traditional payment methods, other digital currencies, or transfers between digital currency owners. Most exchanges are located outside the boundaries of the United States in order to avoid regulation and legal requirements, but some popular exchanges operate inside the jurisdiction of the United States. Binance is an example of a popular online exchange that is located outside of the United States but cooperates with and accepts legal process from American law enforcement agencies.

e. A wallet is a means of storing digital currency identified by unique electronic addresses that allows an individual to conduct transactions on the public ledger. To access a wallet on the public ledger, an individual must use a public address (or "public key") and a private address (or "private key"). The public

address can be analogized to an account number while the private address is similar to a password used to access that account. Even though the public address of those engaging in digital currency transactions are recorded on the public ledger, the true identities of the individuals or entities behind the public address are not recorded. If a real individual or entity is linked to a public address, however, it may be possible to determine what transactions were conducted by that individual or entity. Therefore, digital transactions are often described as "pseudonymous," meaning they are partially anonymous. Most individuals are identified when they use a digital currency exchanger to make a transaction between digital currency and fiat, or through digital currency exchangers that voluntarily or through legal order, cooperate with law enforcement.

f. What is common across many exploitations of the elderly and elder abuse cases when it comes to cryptocurrency, is that they initially contact the victim from a point of perceived authority to the victim. They do this through email, text message, and sometimes computer access through a point of compromise such as a virus or clicking a fraudulent link. This can be as sophisticated as impersonating law enforcement or purporting to be from their bank's corporate security. Once the suspect engages with the victims, they often request that they hide or lie about their actions as to not raise suspicion from actual authorities. From this point, they convince the victim to withdraw their own funds from their accounts and forward it to the suspect through various means. A common method it is to have the victim

deposit cash into a Bitcoin ATM and send the transaction to a wallet address provided to the victim.

g. On or about August 8, 2022, F.W., an 80 year-old resident of Greenville, S.C. received a text message stating she had just purchased a $600.00 Samsung smart phone and that if this was not a purchase she made, to contact the number provided. F.W. contacted the number and spoke with a male named "Neil" who spoke with a deep accent. The person on the phone instructed F.W. that her bank account at Truist Bank had been compromised and that he would help her store it in a secure account while they investigated. He instructed her to travel to her bank and withdraw $20,000.00, and if the teller questioned her, to say that it was for home renovations as he warned that an employee at the bank may be involved in the account being compromised.

h. F.W. traveled to her bank and withdrew $20,000.00 in cash. She was then instructed to go to the Circle K/Marathon gas station at 820 South Church Street and go to a Bitcoin ATM machine. From there she deposited the maximum amount allowable of $15,000.00 and sent it to the cryptocurrency wallet address provided by the scammer. This wallet address is xxxxxxxxxxxxxxxxxxxxxxxxxxxxxK7Zg ("Suspect Wallet 1"). Once the victims sent the BTC to the wallet address provided, the suspect cut off all further communication.

i. Special Agent ("SA") Joseph Lea ("Lea") reviewed transaction history for digital currency wallet Suspect Wallet 1 in a commercial blockchain analysis platform. Below is a summary of his review:

(1) On August 8, 2022, at 21:20:43 hours 0.50069530 BTC was deposited into the wallet via transaction ID: f69438804e58dld7fab4cbb9084741d7d1234eb6f2d5d0f46lffa4a428b6a88b. Based on SA Lea's experience and information from the victim, he believed this deposit was from F.W. and matched the receipt the victim received from the BTC ATM and turned over to the Greenville Police Department.

j. Based on this incident, SA Lea learned that on or about March 4, 2022, B.W., a 76-year-old resident of California was on her home computer with it began to glitch and a message popped up on the screen indicating that her Apple account had been compromised and she needed ·to call in to speak to a security manager. B.W. contacted the number and spoke with a male with a heavy accent. He instructed B.W. that her account had been compromised and that she needed to get her funds into a secure account. At the suspect's direction, she withdrew $10,000.00 dollars and made deposits into Suspects Wallet 1 and another unidentified wallet in two transactions between March 4, 2022 and March 5, 2022.

(1) SA Lea reviewed transaction history for Suspect Wallet 1 in a commercial blockchain analysis platform·. These transactions are detailed below:

0.02595776	18d7edb35eflb151clc729ddb176cl3a61ab9b02f2c73bbd85Sb2ceScac69c09	2022-03-05 19:04:58
0.03295144	0b2947fca2d3b9caceca4316ace44afe9fdc934c29de3c671dae4e8d03e38397	2022-03-05 19:04:57
0.05033321	886c53b7598b9bb0bbbbb2686009aclb4500942b0128ce1473180b8ed8ebefcf	2022-03-05 17:59:02

k. On or about June 23, 2022, M.R., a 72-year-old resident of Pennsylvania was on her home computer when a pop-up advised her that her Wells Fargo account had been compromised and she needed to call in to speak to a security manager. M.R. contacted the number and spoke with the supposed manager. He instructed M.R. that her account had been compromised and that she needed to get her funds into a secure account. At the suspect's direction, she withdrew $10,100.00 dollars and made a deposit at a BTC ATM which deposited into Suspect Wallet 1.

(1) SA Lea reviewed transaction history for Suspect Wallet 1 in a commercial blockchain analysis platform. On June 24, 2022, at 18:14:51 hours 0.42261794 BTC was deposited into the wallet via transaction ID:

e8c4c7af34170f2e7950eld85d518194465c2a53b9fb076b3d58d77cd74dd26d. This matched documentation provided by Hippo Kiosks, which is the BTC ATM hosting company.

(2) When first confronted by Hippo Kiosks, warning about possible elderly scams, M.R. stated that she was using the money to purchase a car. She later recanted and stated that she had been scammed and was instructed by the scammer to say she was buying a car to avoid suspicion.

l. Based on reports filed by several BTC ATM hosting companies, SA Lea learned the following: to date there have been numerous other purported victims of this same type of fraud and that have sent funds to the same Suspect Wallet 1. These BTC ATM hosting companies have jointly reported approximately $500,000.00 worth of possible fraud related to victims sending funds to Suspect Wallet 1.

m. At various times over the past several months, Suspect Wallet 1 received numerous deposits from victims. These transfers constituted the proceeds of wire fraud, money laundering and monetary transaction in criminally derived property.

n. On August 23, 2022, SA Lea reviewed transaction history in Suspect Wallet 1 provided by the hosting exchange, Binance:

(1) Binance identified Avinash Pal as the account holder of Suspect Wallet 1. Between March 4, 2022 and August 8, 2022, Suspect Wallet 1 received 744 deposits totaling approximately $2,318,448.90, and sent 96

transactions totaling approximately $2,335,104.984. Of which, 55 withdrawals totaling $1,991,123.80 USDT go out to wallet xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx7y2G ("Burn Wallet l"). Burn Wallet l[2] is a wallet address on the TRON network, which is known as a "Privacy Coin" and is often used by fraudsters in an attempt to obscure the source, nature, or ownership of the funds. Suspect Wallet 1 also has conducted 500 Over The Counter[3] ("OTC") trades, totaling approximately $1,512,272.94.

(2) As it relates to tracing digital currency stolen from the victims discussed above, on March 5, 2022, between approximately 17:59 and 19:04 UTC, Suspect Wallet 1 received 3 deposits from victim B.W. totaling 0.10924241 BTC valued at approximately $5,000. Approximately 6 minutes later at 19:10 UTC, an OTC transaction occurred selling .05 BTC for approximately $2,328. No immediate withdrawals occurred from Suspect Wallet 1 that same day.

(3) On June 24, 2022, at approximately 18:14 UTC, Suspect Wallet 1 received 1 deposit from victim M.R. totaling 0.42261794 BTC valued at approximately $10,100.00. Approximately 2 minutes later at 18:16 UTC, an OTC transaction occurred selling 0.42261794 BTC for approximately

[2] A burn wallet address is one that is specifically used as an intermediary wallet where the funds come in and are comingled with other funds and then immediately sent out. This is done to further obscure the location, nature, and source of the illicit funds.

[3] OTC trades occur when a user trades coins peer-to-peer. This is often done to obscure the source of the funds and prevent the transaction from showing on the public block chain.

$8,876. The following day the first withdrawal since the OTC sale, at 08:47 UTC, a withdrawal of $52794.99 USDT was made and sent to wallet address xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx7y2G (Burn Wallet 1) The funds were then immediately transferred out through numerous wallets very quickly and comingled with other funds, into an unidentified wallet address.

(4) On August 08, 2022, at approximately 21:20 UTC, Suspect Wallet 1 received 1 deposit from victim F.W. totaling 0.5006953 BTC valued at approximately $15,000.00. Approximately 4 minutes later 21:24 UTC, an OTC transaction occurred selling 0.5006953 BTC for approximately $11,925.87. The following day the first withdrawal since the OTC sale, at 09:26 UTC, a withdrawal of $48,943.35 USDT was made and sent to wallet address xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx7y2G (Burn Wallet 1). The most immediate and direct link was a transfer to wallet address xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxYPqx ("Burn Wallet 2"), where it was comingled with other funds and then immediately transferred to wallet xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxHKhh ("Suspect Wallet 2").

o. Based on SA Lea's training and experience, the agent concluded that Suspect Wallet 1 was used by the Subjects to receive proceeds from victims of wire fraud and to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds obtained from the scam. Suspect Wallet 1 was used to facilitate the commission of the money laundering and monetary transaction in

criminally derived property and Suspect Wallet 1 contained proceeds of the above offenses.

p. The Suspect Wallet 1 bears numerous red flags for a money laundering facilitation account, namely:

(1) The volume of transactions in the Suspect Wallet 1 is highly suspicious, with more than $5 million in USD equivalent of digital currency moved through the wallet associated with the Suspect Wallet 1 in less than a month and a half;

(2) The Suspect Wallet 1 does not appear to hold digital currency for long, instead rapidly receiving and then retransmitting digital currency, and often in the form of stablecoins;

(3) The Suspect Wallet 1 appears to immediately convert via OTC transactions at a loss of value, the original stolen types of digital currency into stablecoins before transferring the resulting digital currency via a privacy network called TRON;

(4) The conversions in the Suspect Wallet 1 appear to lack a business purpose, because the operator(s) of the Suspect Wallet 1 converted more than $2 million in BTC into USDT over numerous transactions, but these conversations have

negative value once the sale is made and any transactions costs are considered;

(5) The Subject Wallet 1 does not appear to be engaged in any investment activity, as digital currency is rapidly moved in and out, and stablecoins are designed not to increase in value greater than the USD;

(6) While these amounts might be unsurprising in a commercial or business account, the Suspect Wallet 1 was opened as a personal account with no identified associated business;

(7) Public information searches for PAL do not identify any legitimate businesses associated with PAL which would justify a personal account receiving and sending these volumes of digital currency; and

(8) The transaction activity in the Suspect Wallet 1 appears consistent with a "layering" account in a money laundering scheme, where an account is used primarily to receive and convert criminal proceeds before transmitting the proceed on to another recipient, thus disguising the source of the proceeds and frustrating asset recovery and law enforcement.

q. Based on SA Lea's investigation, records provided by Binance, and Special Agent Lea's training and experience, the government believes Suspect Wallet 1 was used by Avinash Pal primarily to receive proceeds of elderly abuse scams involving digital currency stolen from victims and to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds obtained from the scam. The Suspect Wallet 1 was used to facilitate the commission of the Subject Offenses, contains proceeds of the Subject Offenses of BTC and USDT (the Subject Funds) are subject to seizure and forfeiture.

r. A federal seizure warrant was executed for the Suspect Wallet 1, under the control of Binance, on September 01, 2022 by SA Lea.

8. Based on the information and allegations set forth herein, there is a factual basis to support a reasonable belief that the Government will be able to meet its burden of proof at trial to show that the Defendant Funds constitutes, or is traceable to:

b. property involved in wire fraud transactions or attempted wire fraud transactions in violation of 18 U.S.C. § 1343

b. property involved in money laundering transactions or attempted transactions in violation of 18 U.S.C. § 1956(a)(1)(A)(i), and/or § 1956(a)(1)(B)(i) and/or 1957;

c. property involved in an illegal money transmitting business, in violation of 18 U.S.C. § 1960; and/or

d. proceeds of some other form of specified illegal activity set forth in 18 U.S.C. § 1956(c)(7) and;

e. proceeds of some other form of specified illegal activity set forth in 18 U.S.C. § 1956(h) and;

f. property involved in money transactions in criminally derived property, in violation of 18 U.S.C. § 1957.

CONCLUSION

10. By reason of these premises, and pursuant to 18 U.S.C. § 981(f) and 21 U.S.C. § 881(h), whereby the Plaintiff's right, title and interest in and to the Defendant Funds relates back to the commission of the act giving rise to the forfeiture, the Defendant Funds has become and is forfeited to the United States of America, to be disposed of pursuant to Supplemental Rule G(7)(c) for Admiralty or Maritime Claims and Asset Forfeiture Actions, 18 U.S.C. § 981(d), 21 U.S.C. § 881(e), and other applicable laws.

WHEREFORE, Plaintiff prays that due process issue to enforce the forfeiture of the Defendant Funds, *in rem*; that a Warrant for the Arrest of the Defendant Funds be issued; that due Notice be given to all interested persons to appear, make claim, answer and show cause why the forfeiture should not be decreed; that the Defendant Funds be decreed condemned and forfeited to the United States of America for disposition according to law; and that Plaintiff have such other and further relief as the Court may deem just and proper, together with the costs and disbursements of this action.

Respectfully submitted,

Adair F. Boroughs
UNITED STATES ATTORNEY

By: *s/Carrie Fisher Sherard*
Carrie Fisher Sherard #10134
Assistant United States Attorney
55 Beattie Place, Suite 700
Greenville, SC 29601
(864) 282-2100

September 26, 2022